Jeff Welton
Sales Manager, Eastern USA
Nautel

IT Security in a Virtualized World

SBE

nautel
AM/FM Radio Transmitters

https://securityaffairs.co › wordpress › cyber-crime › si...

Sinclair TV stations downtime allegedly caused by a ...

Oct 18, 2021 — A **ransomware attack** is likely the cause of recent downtime for TV stations owned by Sinclair Broadcast Group **broadcast television** company.

https://www.toledoblade.com › 2021/10/27 › stories

Ransomware attack continues to plague WNWO-TV, Channel 24

Oct 27, 2021 — A local **television** station intermittently **broadcast** a technical-difficulty message Wednesday while its parent company continued to grapple ...

https://www.tvyvideo.com › ... › Enterprises

Colombian TV Channel Attacked with Ransomware | TVyVideo

May 24, 2022 — Canal de **televisión** colombiano fue atacado con **ransomware** ... which was intended to affect the Caracol News system, BLU **Radio** and other ...

https://www.cyberpolicy.com › cybersecurity-education

San Francisco's Public Radio Station Hit by Ransomware

One of the most common cybersecurity challenges plaguing private businesses right now is the **ransomware attack**. Take for instance, San Francisco's public **TV** ...

https://www.radioworld.com › radio-it-management

Marketron Plans Re-Rollout After Ransomware Attack

Sep 23, 2021 — He has interviewed directors of engineering, FCC chairs, national **radio** personalities and corporate executives about digital **radio**, connected ...

https://podcasts.apple.com › podcast › ransomware-and...

why we all need to be ready for cyber attacks Radio Davos

As online working durged during the pandemic, so did cybercrime - **ransomware attacks** rose 151% in 2021. The World Economic Forum's Global Cybersecurity ...

https://omny.fm › shows › kcbsam-on-demand › ranso...

Ransomware attack targeting public schools, here's what to ...

Sep 8, 2022 — There's a **ransomware attack**, this time targeting public schools. For more, KCBS **Radio's** Jim Taylor gets the details from the FBI.

https://www.tampabay.com › breaking-news › radio-sta...

Radio station WMNF victim of ransomware cyberattack

Jul 17, 2019 — Public **radio** stations have been targeted. In 2017, San Francisco NPR station KQED was hobbled for months by an **attack** that forced one of the ...

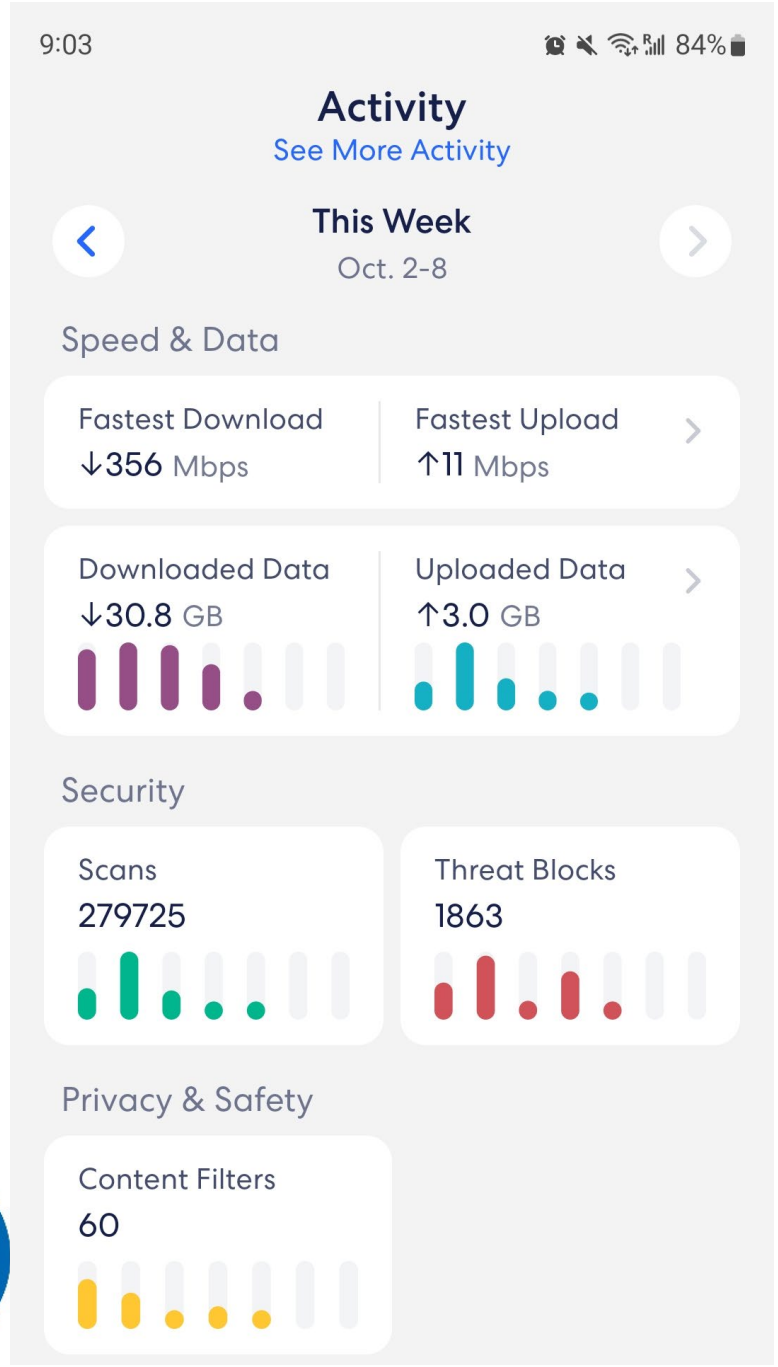
https://www.bbc.co.uk › ... › Drama › Red and Blue

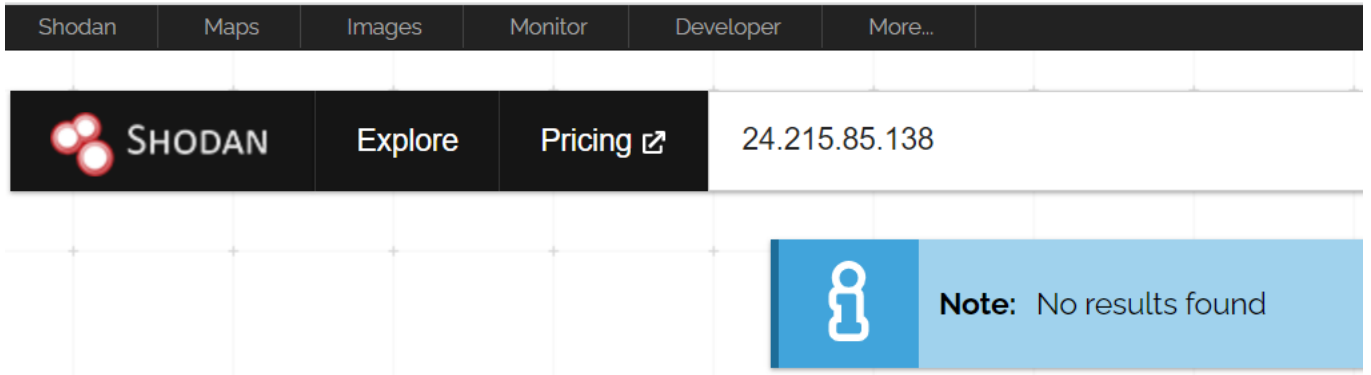
Drama, Red and Blue, Ransomware - BBC Radio 4

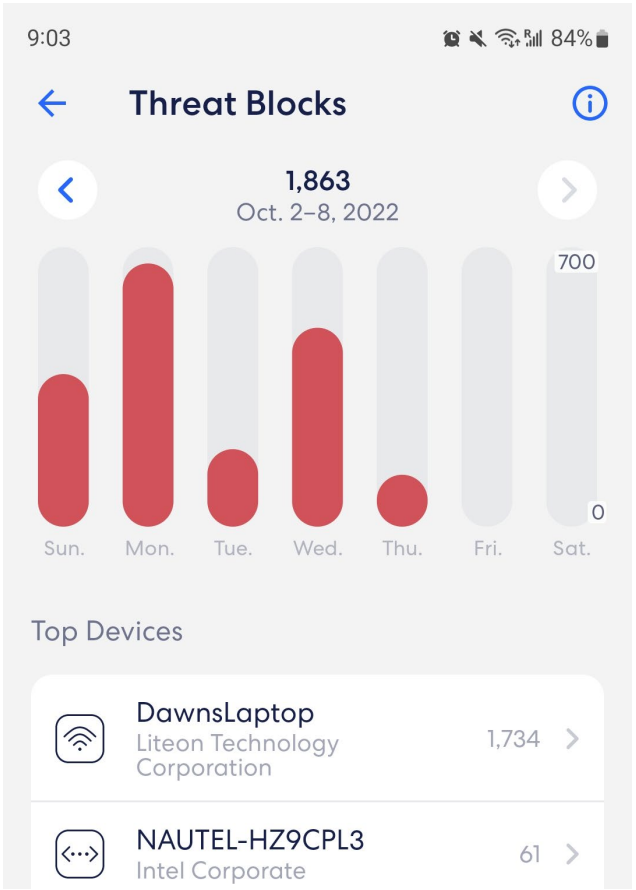
Related Links · Read an article about a war game on Wall Street (www.nbcnews.com) · Is the UK doing enough to protect itself from cyber **attack**? · 'Are you a code ...

SBE.

TRANSMISSION TALK TUESDAY







SBE.

TRANSMISSION TALK TUESDAY

SHODAN Explore Downloads Pricing Nautel

TOTAL RESULTS

14

View Report View or

Product Spotlight: Keep

SHODAN Explore Downloads Pricing Barix

TOTAL RESULTS

1,434

View Report View

Partner Spotlight: Look

SHODAN Explore Downloads Pricing Gatesair

TOTAL RESULTS

3

View Report View c

Access Granted: Want t

SHODAN Explore Downloads Pricing Elenos

TOTAL RESULTS

30

View Report View

Product Spotlight: We'

SHODAN Explore Downloads Pricing Worldcast

TOTAL RESULTS

34

View Report View on

Access Granted: Want to g

SHODAN Explore Downloads Pricing Telos

TOTAL RESULTS

26

View Report Bro

Partner Spotlight: Lo

SBE.

TRANSMISSION TALK TUESDAY

Open **Ports**

22 | 80 | 161 | 443

nautel

Active Preset: [redacted]

[redacted] FM 102.30 FM - 402 W

07 Sep 2024 - 08:18:28

Remote | Local | 402 W | 17.0 W | 87.3 °F | 96.7 % | RF On | RF Off | 1

nautel

Active Preset: Normal 1

[redacted] 100.70 FM - 314 W

07 Sep 2024 - 09:31:46

Remote | Local | 313 W | 0.57 W | 70.2 °F | 99.7 % | RF On | RF Off

nautel

Active Preset: Preset 1

93.30 FM - 341 W

07 Sep 2024 - 09:36:21

Remote | Local | 341 W | 3.58 W | 64.9 °F | 52.2 % | RF On | RF Off

nautel

Active Preset: Preset 1

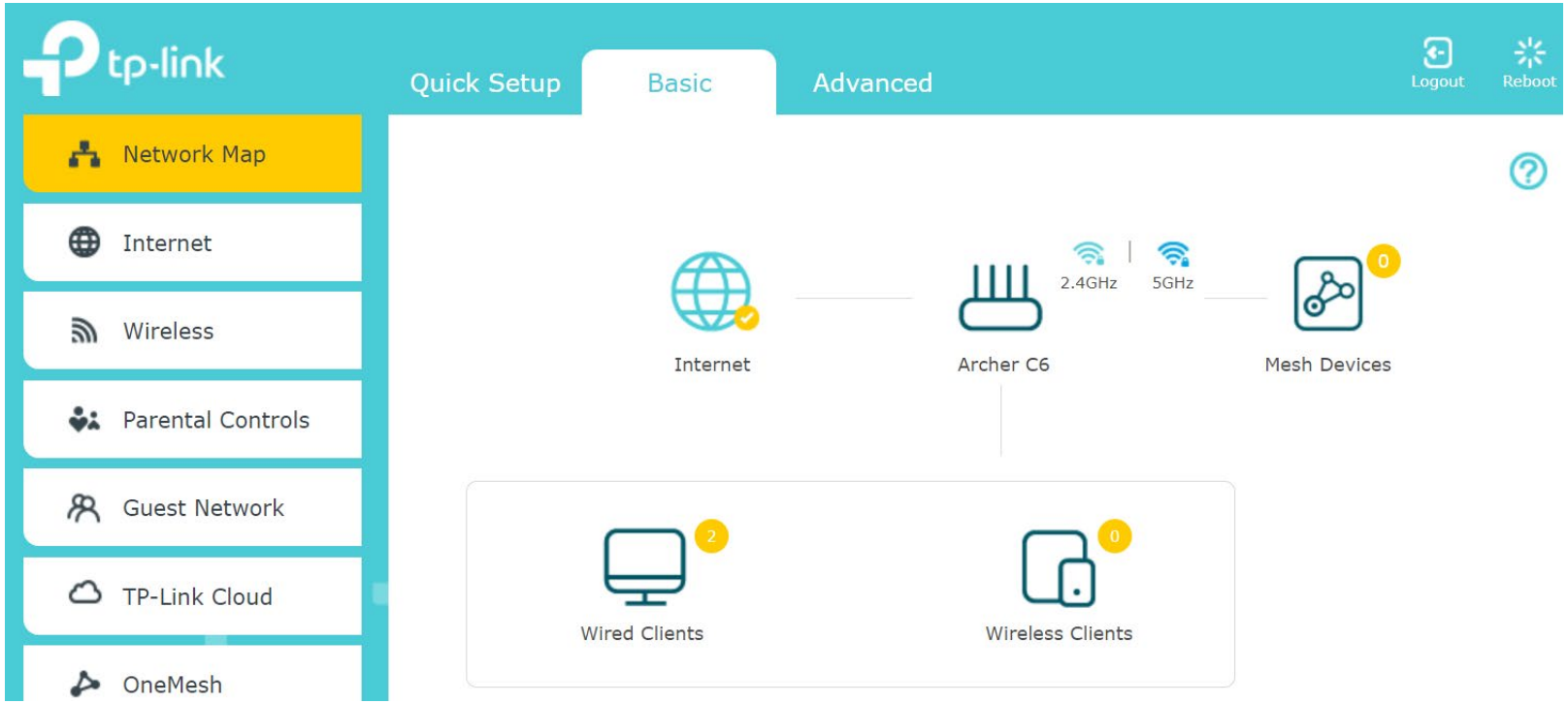
[redacted] 88.70 FM - 500 W

07 Sep 2024 - 07:45:35

Remote | Local | 499 W | 0.08 W | 63.5 °F | 97.2 % | RF On | RF Off

SBE.

TRANSMISSION TALK TUESDAY


tp-link
Quick Setup
Basic
Advanced
Logout
Reboot
Network Map
Internet
Wireless
Parental Controls
Guest Network
TP-Link Cloud
OneMesh
Internet
2.4GHz
5GHz
Archer C6
0
Mesh Devices
2
Wired Clients
0
Wireless Clients

HOME | LOCATION | CONFIGURATION | DEFAULTS | UPDATE | REBOOT

Studio Transmitter Link

Site Type: Studio Encoder
Stream Mode: Never
Keep-Alive: Passive

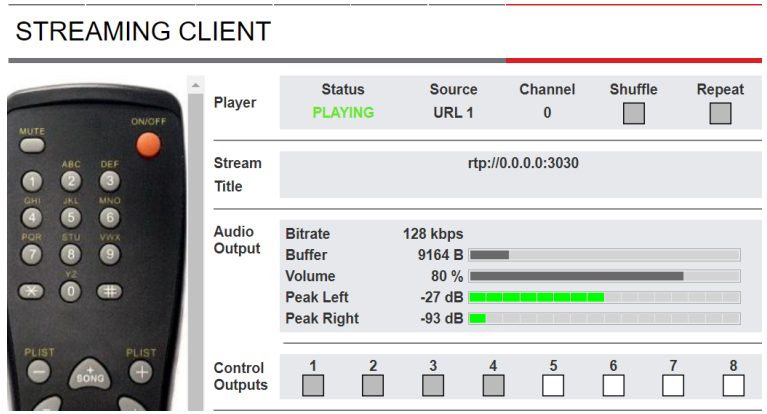
Connection Status: Established FROM [redacted]
Incoming Stream Status: OFF
Outgoing Stream Status: OFF

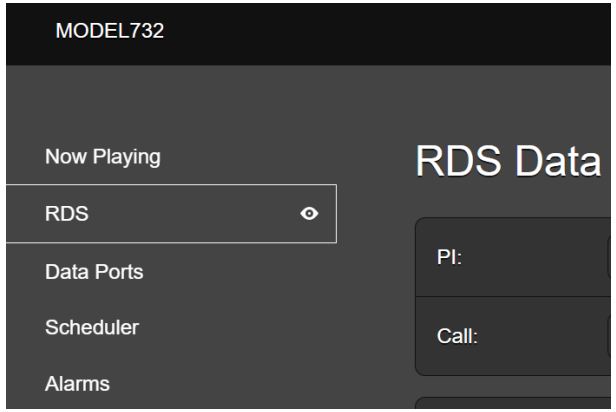
Audio Input: Line Stereo
Audio Format: PCM 16bit mono big endian 24 kHz

Input Audio Level (L): -14 dBFS
Input Audio Level (R): -13 dBFS
Output Audio Level (L): -93 dBFS
Output Audio Level (R): -93 dBFS

Relay 1: always OFF
Relay 2: always OFF
Relay 3: always OFF
Relay 4: always OFF

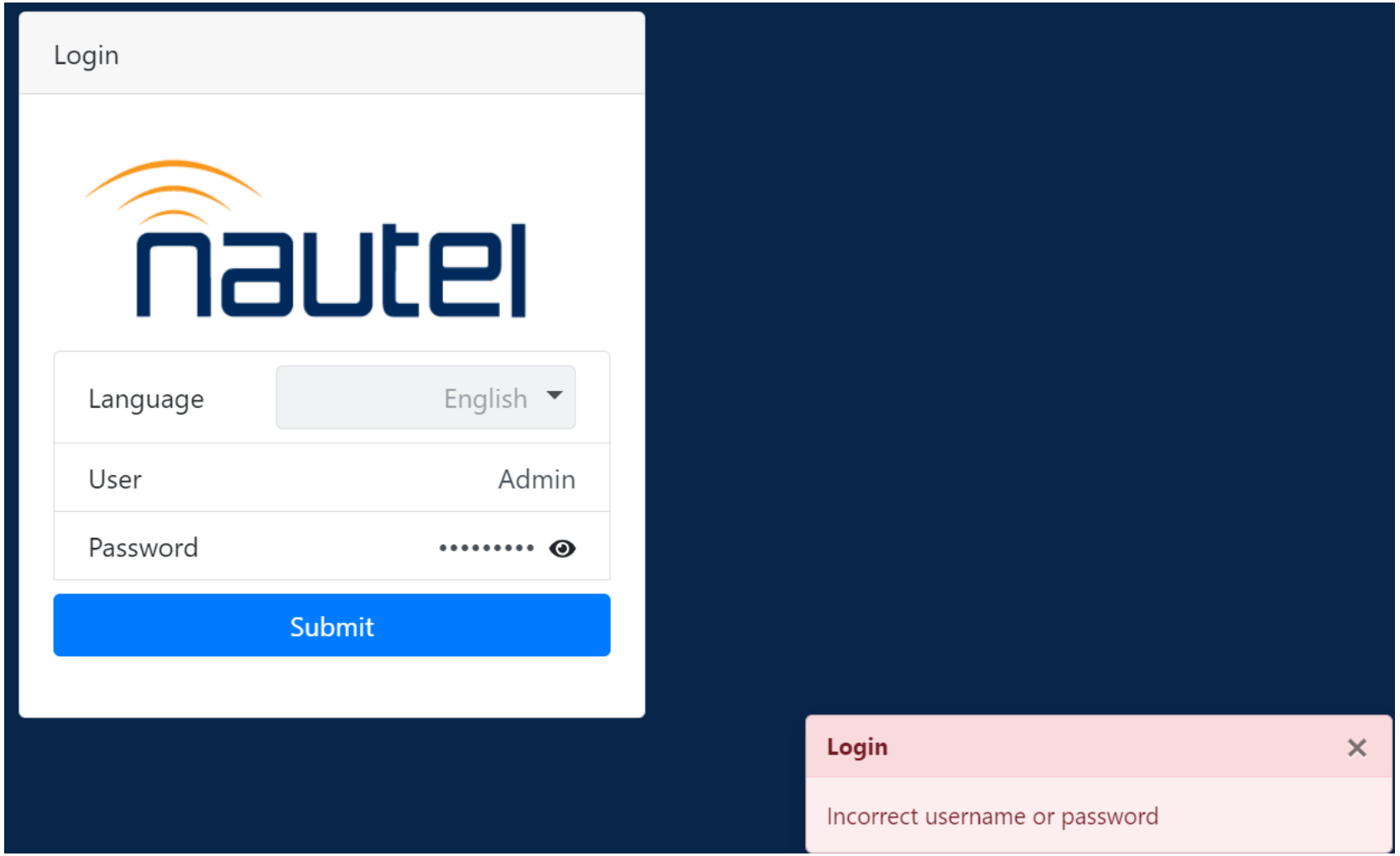
Remote Inputs:
Local Inputs:
Local Relays:





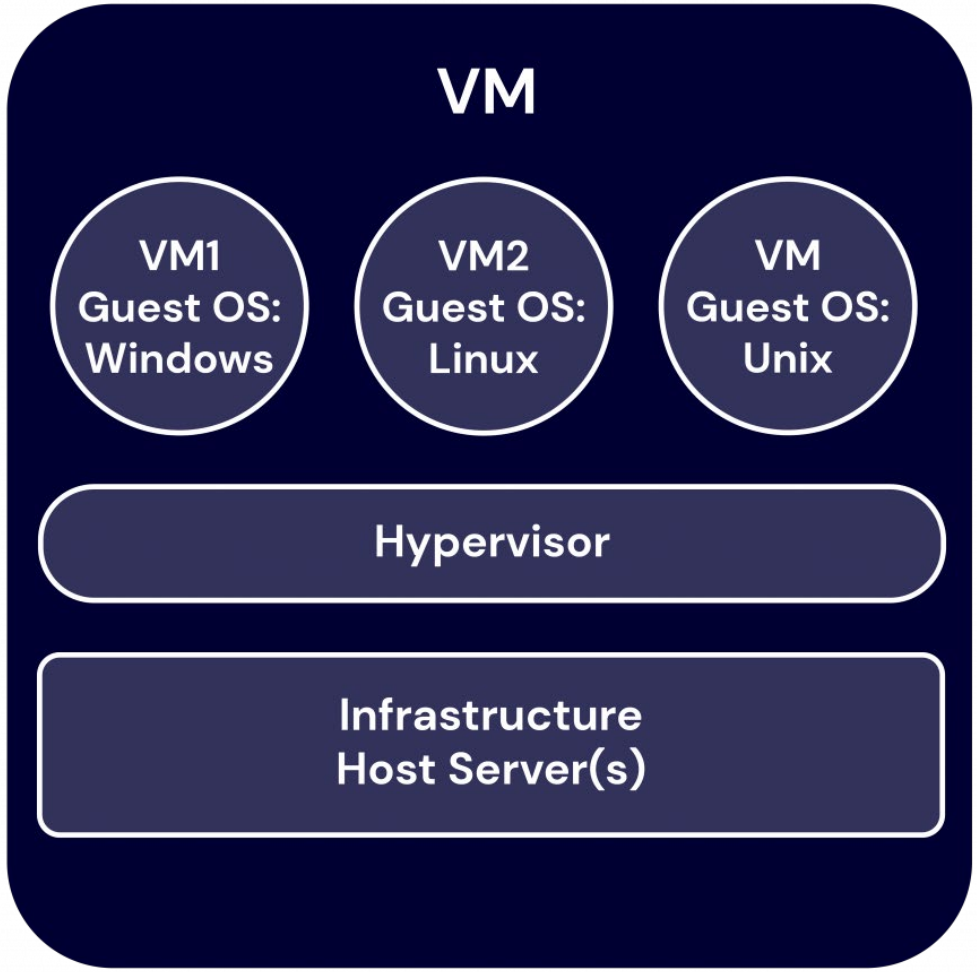
SBE.

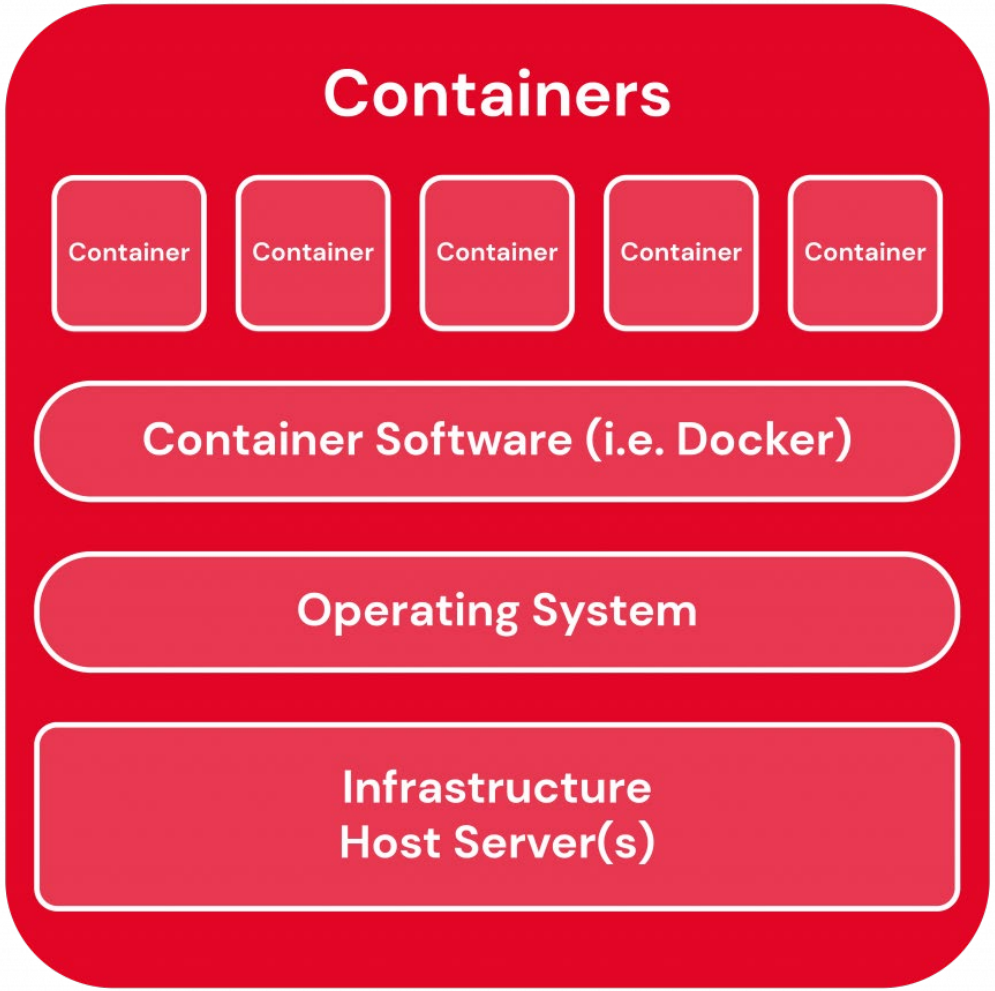
TRANSMISSION TALK TUESDAY



SBE.

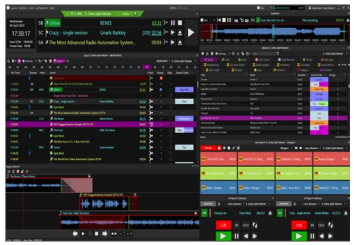
TRANSMISSION TALK TUESDAY





https://www.backblaze.com/blog/vm-vs-containers/

How did HD Radio get so Complicated?



Codec TX

Codec RX

Studio

IP STL

Transmitter

FM Audio Processor

HD1 Audio Processor

RX Diversity Delay Correction delay

HD MULTICAST+ IMPORTER/EXPORTER

GPS

nautel

MPX

E2X

Codec TX

Codec TX

Codec TX

Codec RX

Codec RX

Codec RX

HD2 Streaming Processor

HD3 Streaming Processor

HD4 Streaming Processor

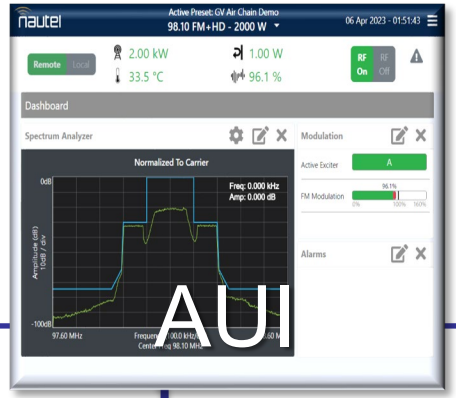
HD2-4 need processors, more STL capacity

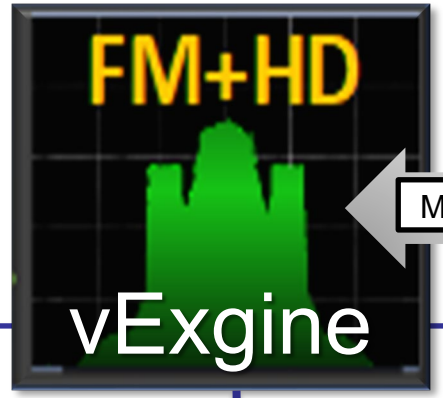
SBE.

TALK TUESDAY

Virtual Architecture

JUST ADD AUDIO





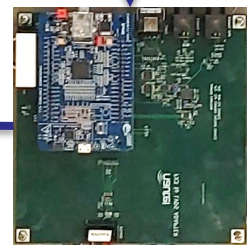
MPX E2X

Controller CPU

Exciter

PROXMOX

Virtualization Engine



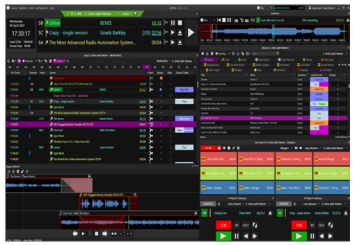
IQ Exciter Interface

GV² Hardware Platform

SBE.

TRANSMISSION TALK TUESDAY

Step 3: Introducing … GV²



Studio

IP STL

Transmitter

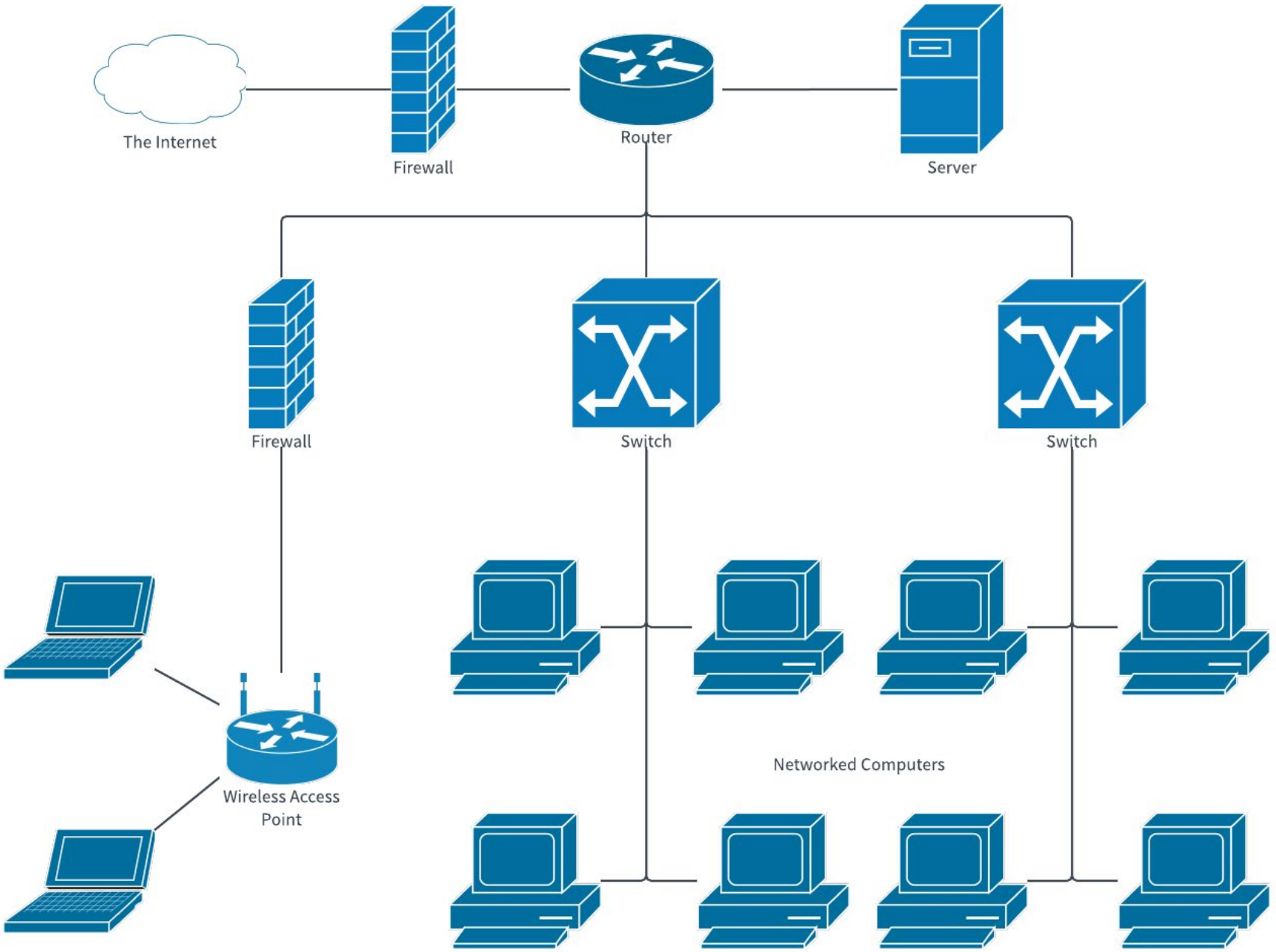
JUST ADD AUDIO

Livewire

Integrated HD
Audio Processing
STL solution

SBE

TALK TUESDAY



https://www.edrawmax.com/network-diagram/how-to-draw-a-network-diagram/

RIPR IP Address Schema - public copy

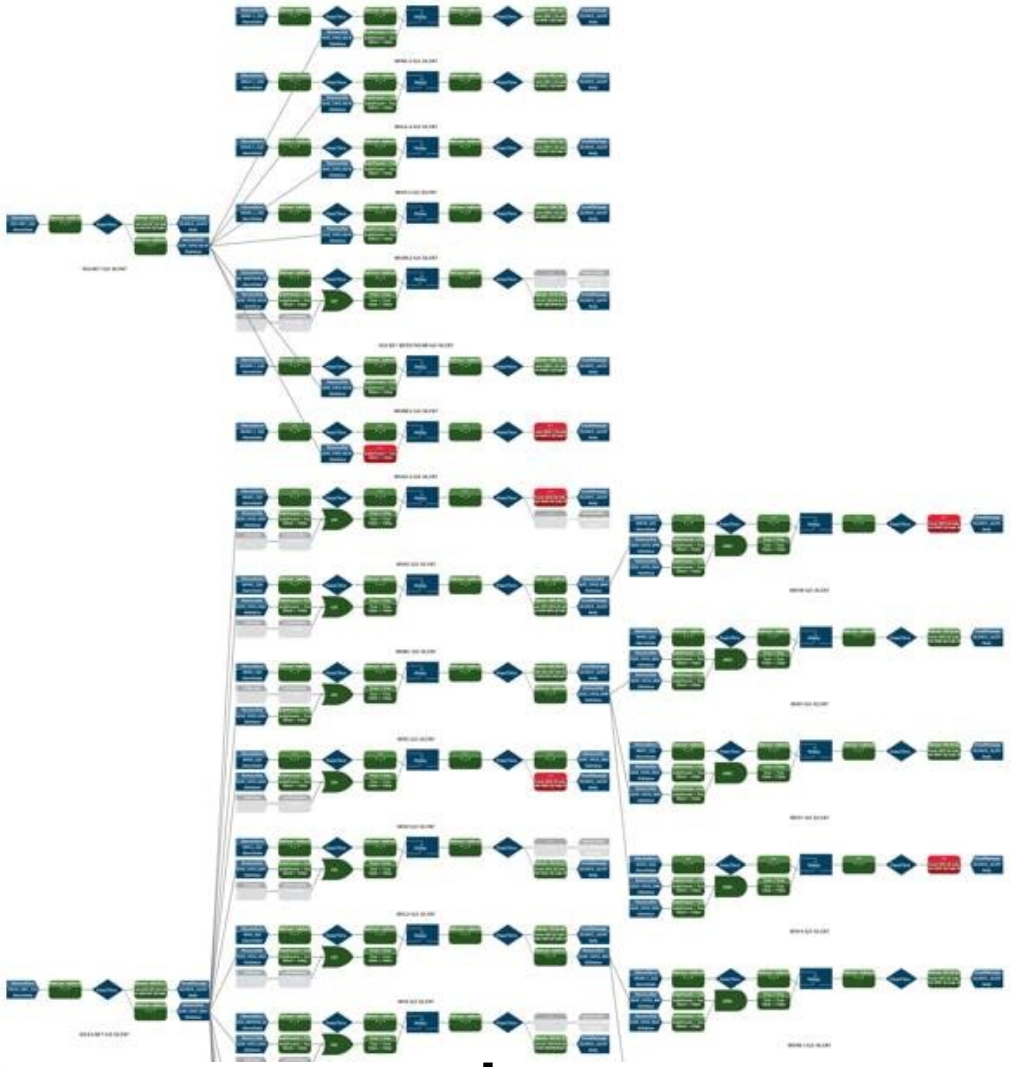
File Edit View Insert Format Data Tools Add-ons Help Last edit was made yesterday at 2:10 PM by Tech RIPR

A1 Location

	A	B	C	D	E	F	G	H	I	U
1	Location	ISP	IP	SUBDOMAIN	DESCRIPT	GATEWAY	MASK	DNS1	DNS2	
2	1 Union Stn	OSHEAN	1		ABS-managed Barracuda	.17	255.255.255.240	71	72	
3	1 Union Stn	OSHEAN	1			.17	255.255.255.240	71	72	
4	1 Union Stn	OSHEAN	1		iPort1US	.17	255.255.255.240	71	72	
5	1 Union Stn	OSHEAN	1	on.org	89.3 IP Codec ETH0	.17	255.255.255.240	71	72	
6	1 Union Stn	OSHEAN	1		89.3 UMD BRIC Link II	.17	255.255.255.240	71	72	
7	1 Union Stn	OSHEAN	1	on.org	88.1 IP Codec	.17	255.255.255.240	71	72	
8	1 Union Stn	OSHEAN	1	npn.org	102.7 IP Codec	.17	255.255.255.240	71	72	
9	1 Union Stn	OSHEAN	1		No.PVD Bkup BRIC Link II	.17	255.255.255.240	71	72	
10	1 Union Stn	OSHEAN	~~1~~	org	~~Telos Z/IPstream webcast~~	.17	255.255.255.240	71	72	
11	1 Union Stn	OSHEAN	1		StudioB BRIC Link II	.17	255.255.255.240	71	72	
12	1 Union Stn	OSHEAN	1		89.3 HD2 BRIC Link II	.17	255.255.255.240	71	72	
13	1 Union Stn	OSHEAN	1	g	Comrex Access	.17	255.255.255.240	71	72	
14	1 Union Stn	OSHEAN	1			.17	255.255.255.240	71	72	
15	1110 Douglas	OSHEAN	1	n.org	1290 WAN x3	.129	255.255.255.240	71	72	
16	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
17	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
18	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
19	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
20	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
21	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
22	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
23	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
24	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
25	1110 Douglas	OSHEAN	1			.129	255.255.255.240	71	72	
26										

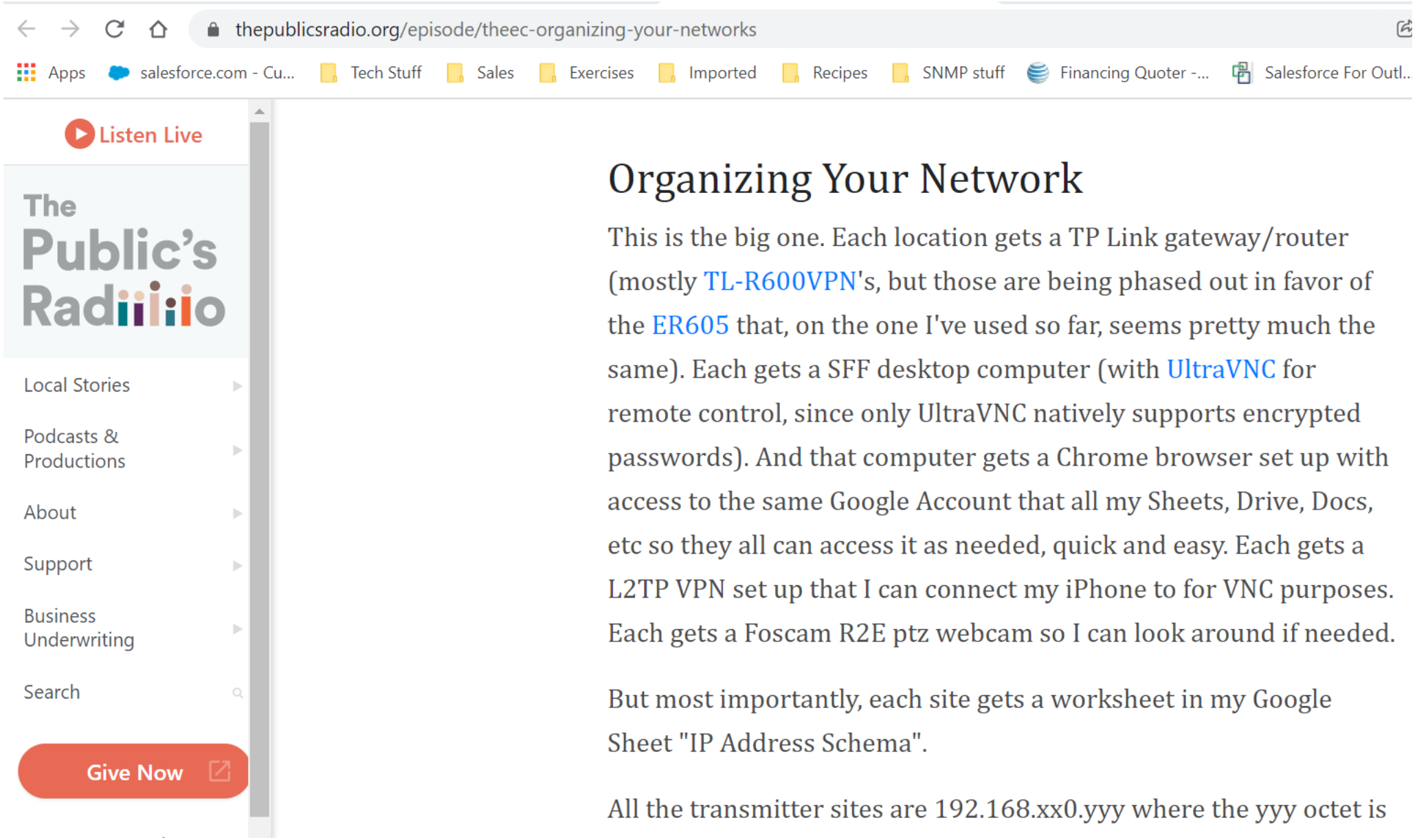
SBE.

TRANSMISSION TALK TUESDAY



SBE.

TRANSMISSION TALK TUESDAY

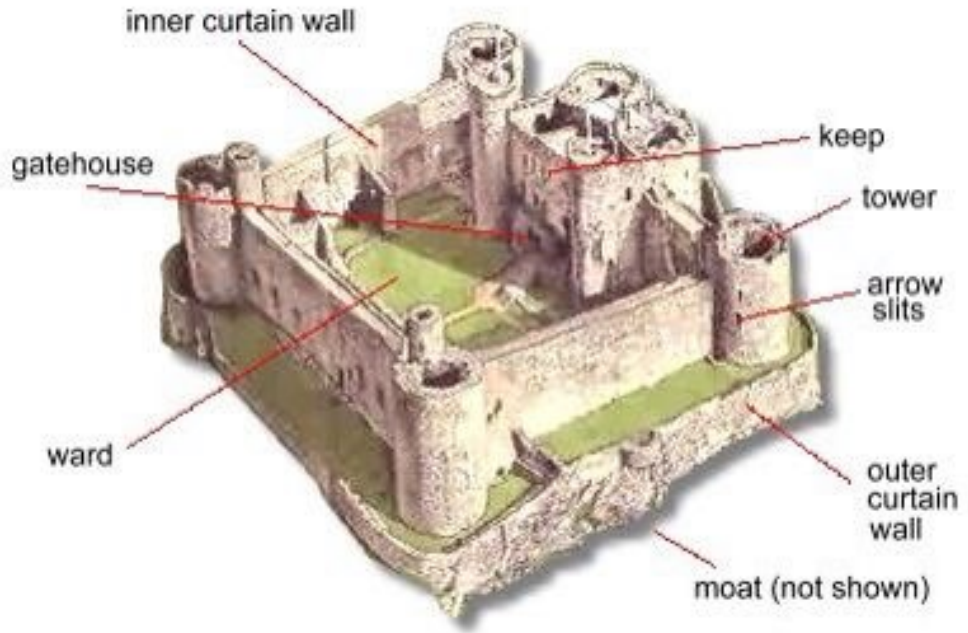


SBE.

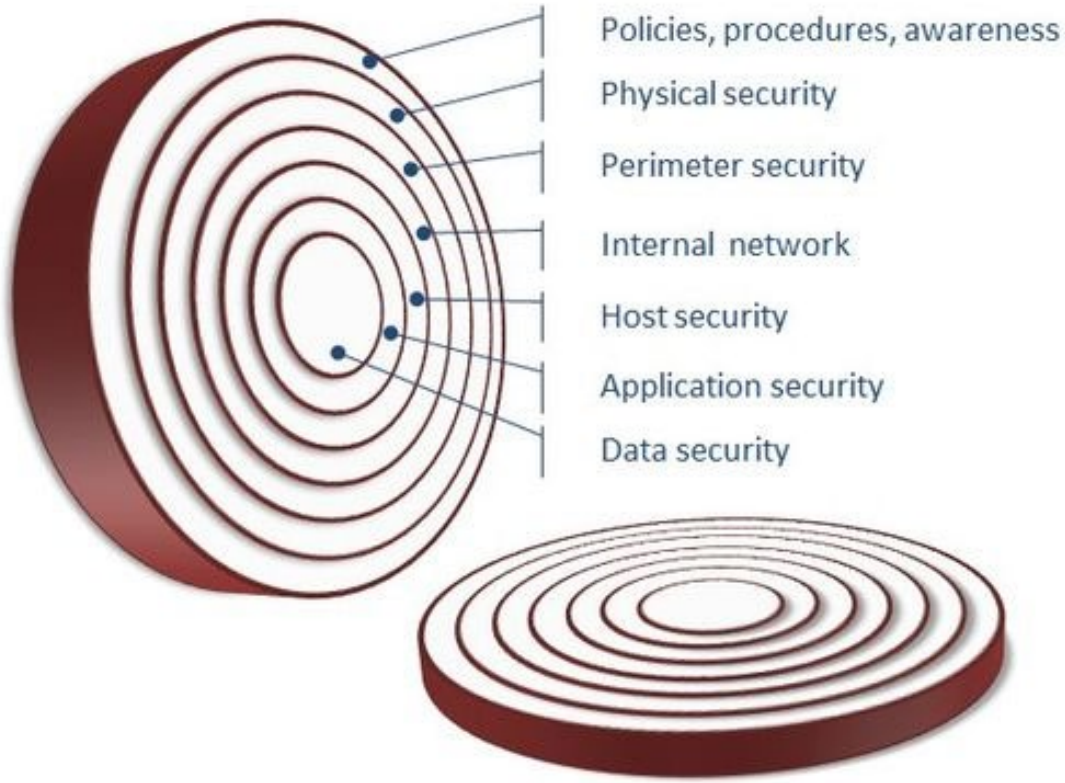
TRANSMISSION TALK TUESDAY

Security Zones

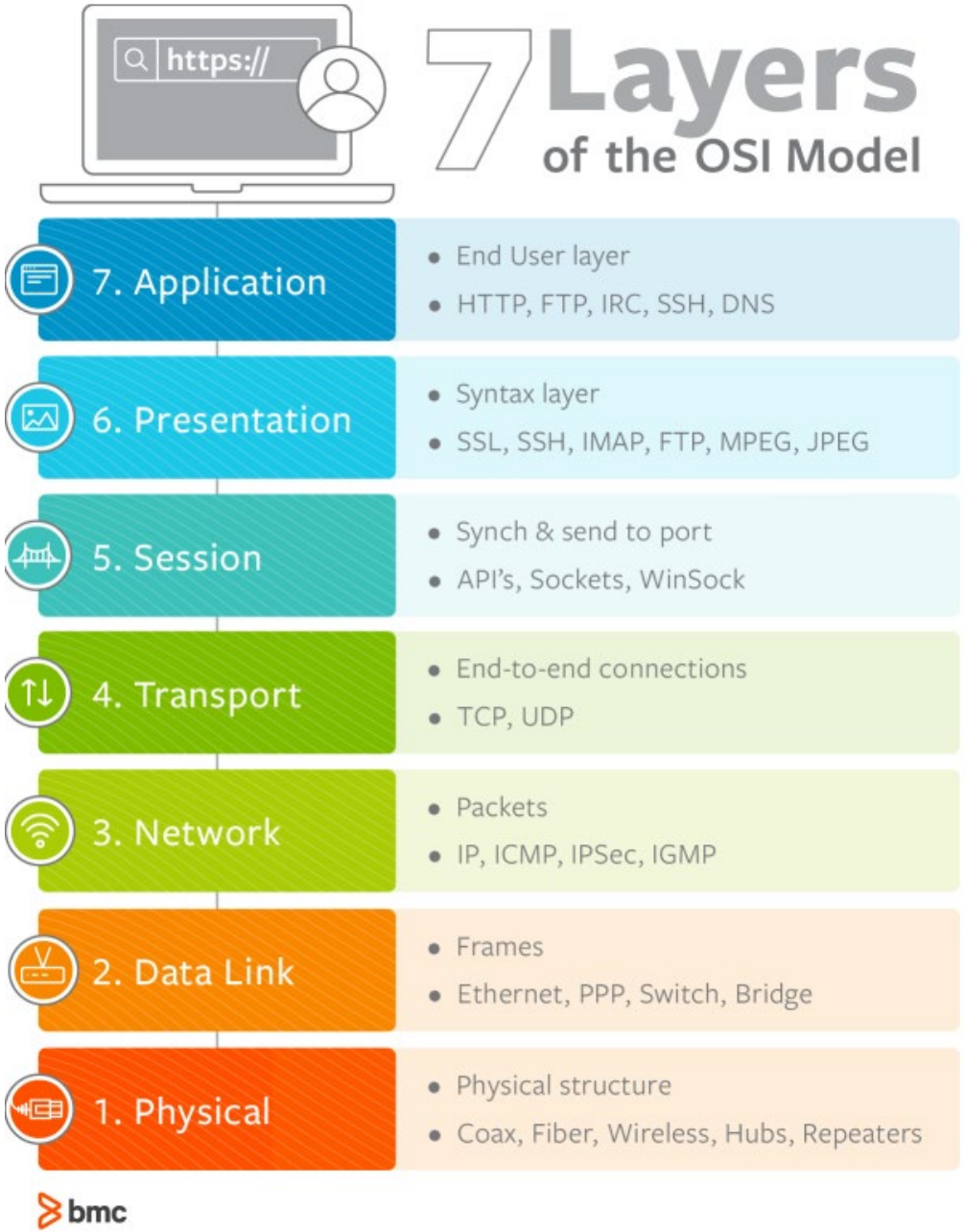
Segmented Network Architecture



Harlech Castle, North Wales, built in 1283 AD



The “Onion Approach”



https://www.bmc.com/blogs/osi-model-7-layers/

Photo from Crawford Media Group's January engineering newsletter

The best security in the world is of no use if the doors are unlocked when the intruder comes calling.

SBE.

TRANSMISSION TALK TUESDAY

Do These 10 Things

Essential

- Change default logins
- Use strong passwords (paraphrases)
- Separate Admin & User accounts on hosts (WIN)
- Segment your network (VLAN) – create multi-layer security zones
- Use packet filtering to control host access (ACL and/or firewall)
- Disable un-used services – close ports not used
- Monitor your network – know what is normal
- Use secure access (SSH not telnet)
- Use VPN for off-site access
- Don’t be a social engineering victim – educate users

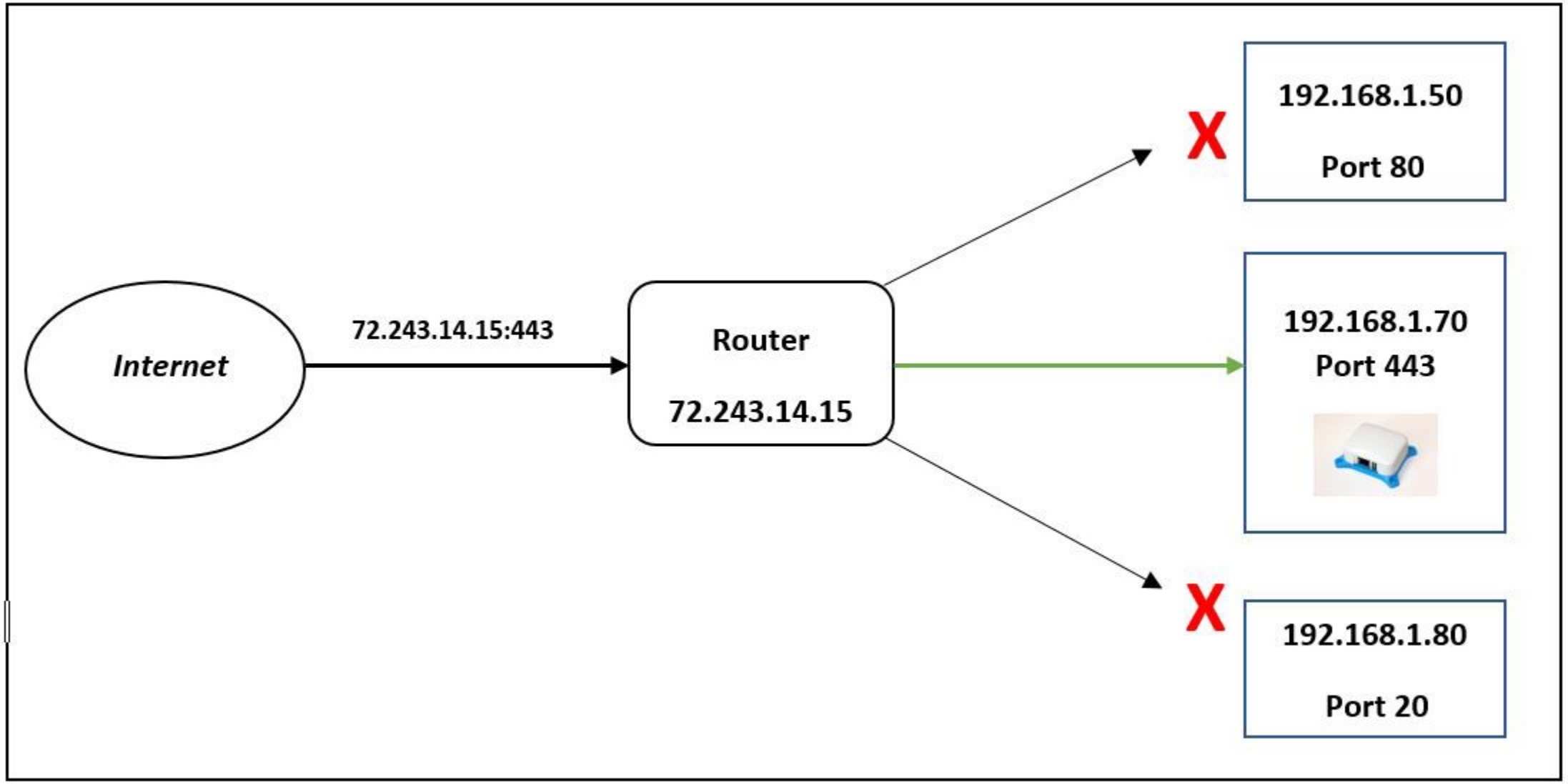
SBE.

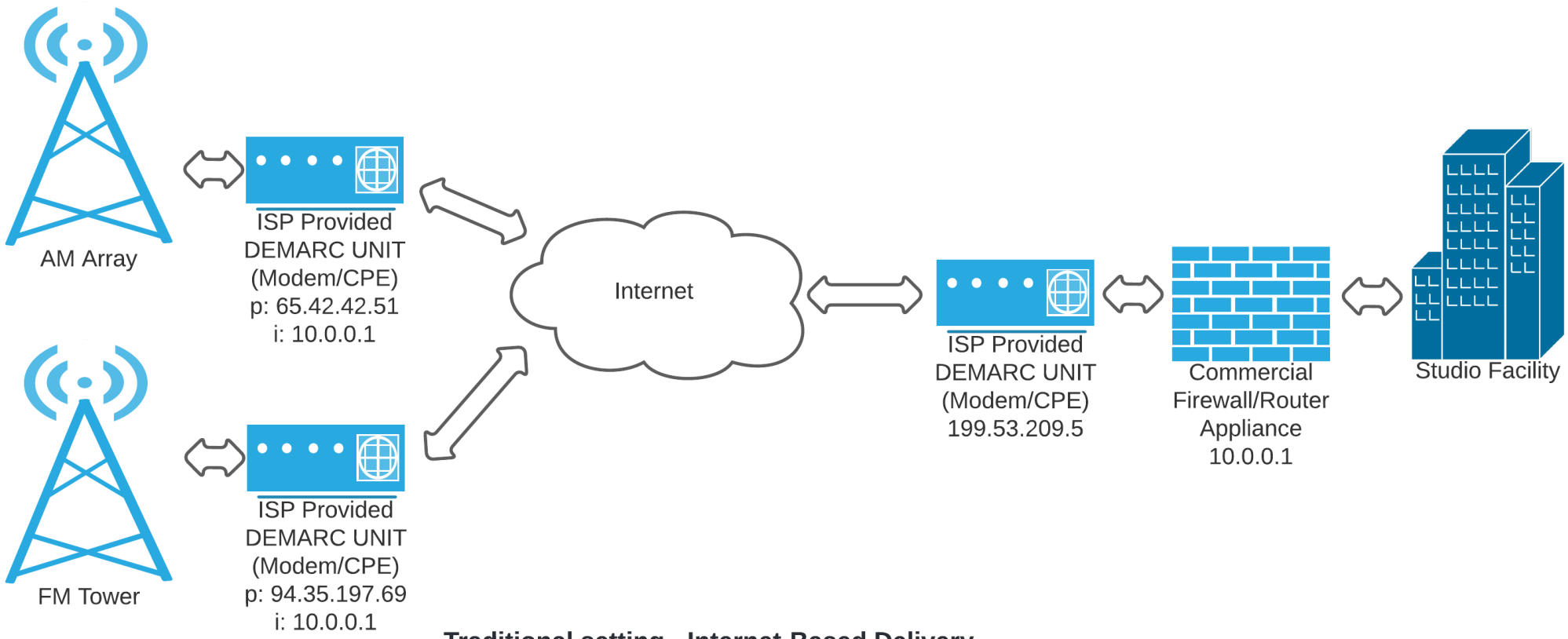
TRANSMISSION TALK TUESDAY

Centrally managed security

"Your device is temporarily blocked from synchronizing using Exchange ActiveSync until your administrator grants it access."

Zero Trust vs. BYOD


Internet
72.243.14.15:443
Router
72.243.14.15
X
192.168.1.50
Port 80
192.168.1.70
Port 443
X
192.168.1.80
Port 20

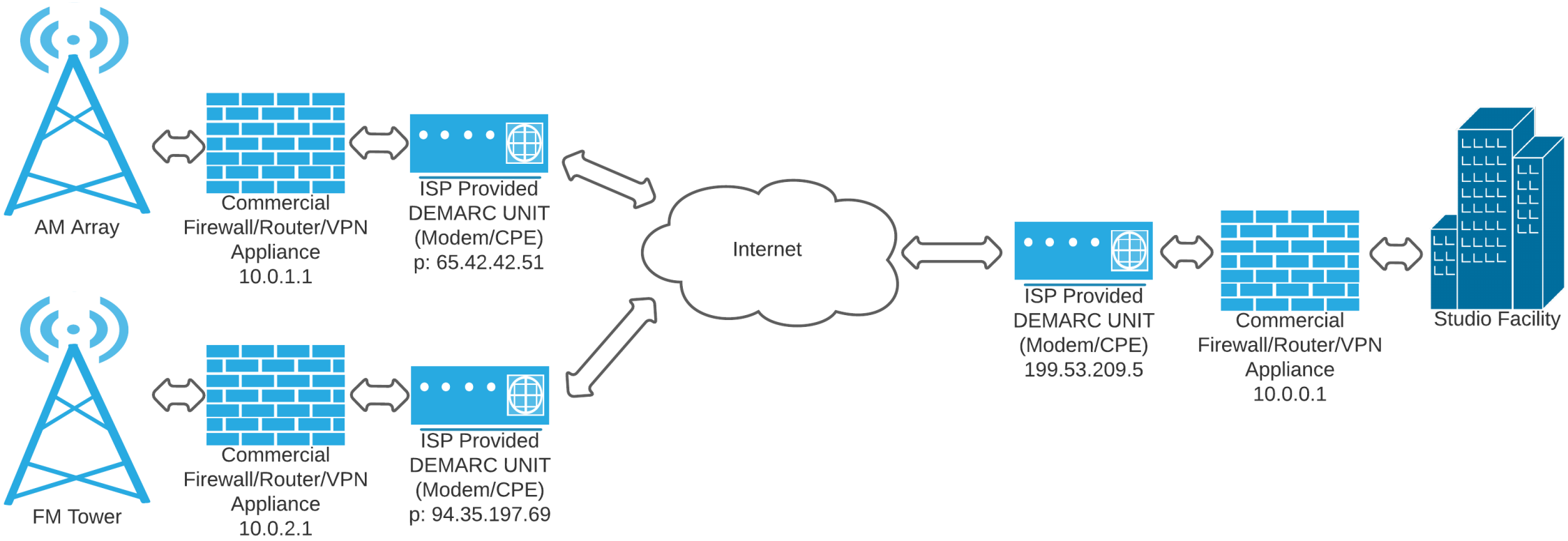


Traditional setting - Internet-Based Delivery

Punch holes through firewalls to deliver audio
Punch holes through firewall to get telemetry
Punch holes through firewall for remote access

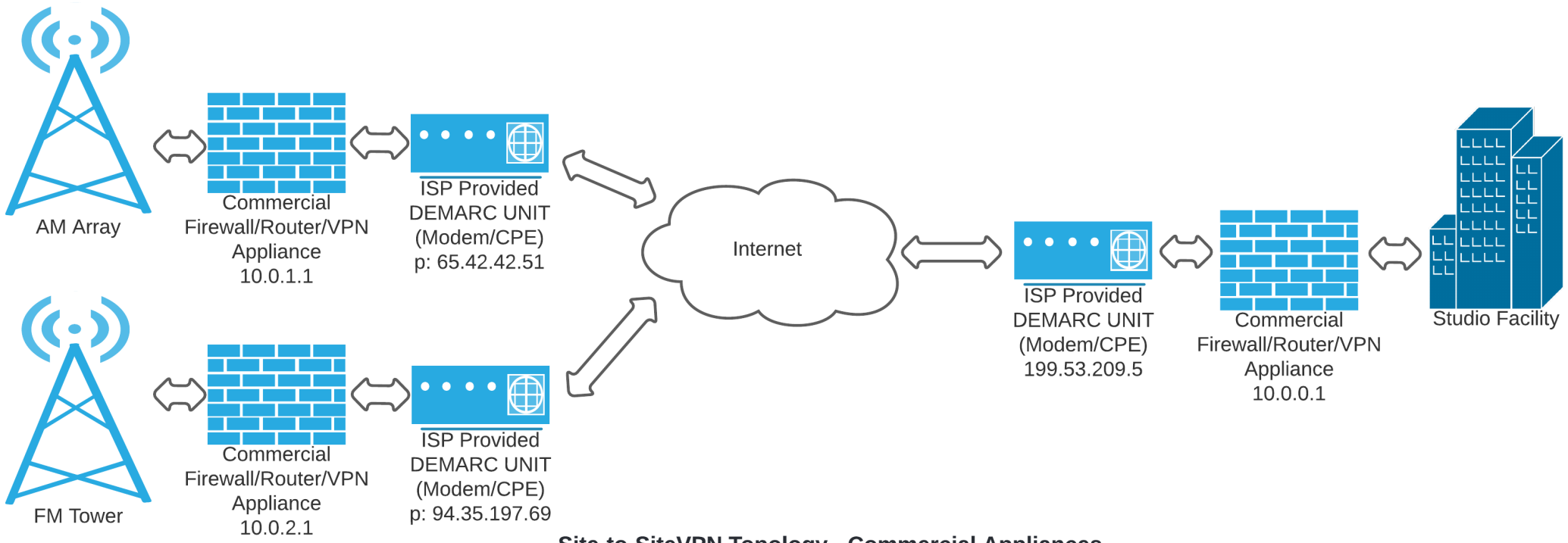
DON'T DO THIS!

https://www.lucidchart.com/pages/



Site-to-SiteVPN Topology - Commercial Appliances

All Internet Traffic through VPN tunnels
No externally visible ports
All traffic is inspected by the home firewall if internet access is required (No "Split-tunnel")
All sites authenticated

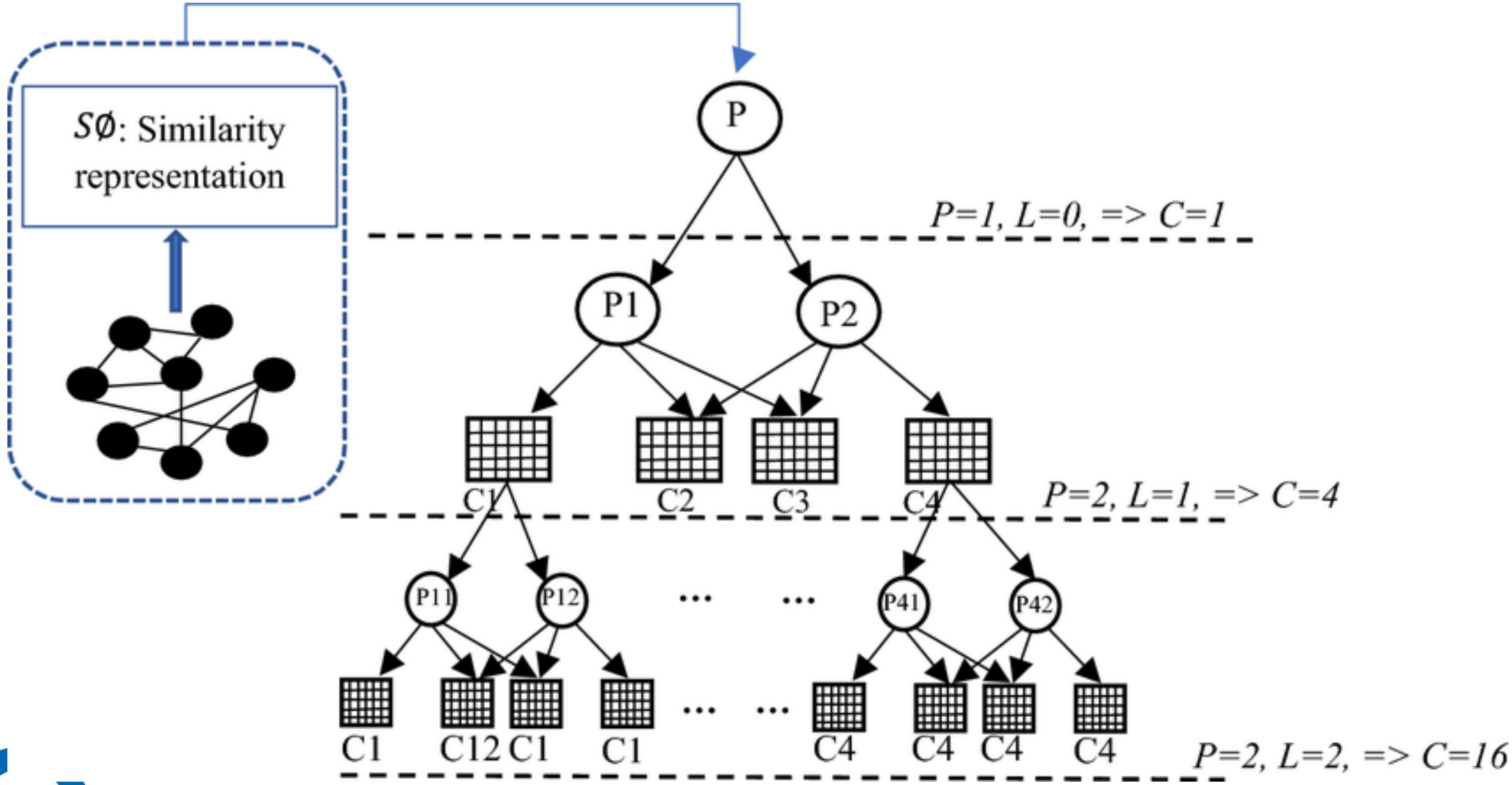


Site-to-SiteVPN Topology - Commercial Appliances

Studio IP: 199.53.209.5
Inside network: 10.0.0.1/24
VPN Tunnel IP to FM: 10.254.253.1/30
VPN Tunnel IP to AM: 10.254.252.1/30

FM Tower IP: 94.35.197.69
Inside network: 10.0.2.1/24
VPN Tunnel IP: 10.254.253.2/30

AM Array IP: 65.42.42.51
Inside network: 10.0.1.1/24
VPN Tunnel IP: 10.254.252.2/30



https://www.researchgate.net/figure/The-process-of-complex-network-partitioning-into-chunks-on-different-levels_fig2_343348595

Hardware

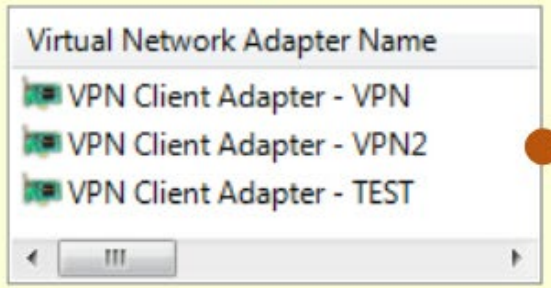
Ethernet Adapter

Ethernet Cable

Ethernet Switch

Virtualization with SoftEther VPN

Software



VPN Tunnel

Virtual Hub Name	Status	Sessions	MAC Tables	IP Tables
BEIJING_SEGMENT	Online	0	0	0
CHINATEST	Online	2	0	0
moosta	Online	3	3	5
Okkota	Online	0	0	0
SoftEther Network	Online	20	474	430
TEST1	Online	0	0	0
UT	Online	0	0	0
VLAN	Online	3	514	2

Virtual Ethernet Adapter

VPN Session over TCP / UDP

Virtual Ethernet Switch (Virtual Hub)

SBE.

TRANSMISSION TALK TUESDAY

Pros of HW

- Appliance based - Usually can have some kind of support contract
- Dedicated hardware
- Multiprotocol support

Cons of HW

- Can be limiting in advanced network topologies
- Cheaper units cannot support lots of remote sites/users
- Can sometimes require a separate authentication system to maintain

Pros of SW:

- Configurable, multiprotocol support
- Installation can be quite simple
- Easy to rollback using snapshots (if enabled, different webinar)
- Can be locked down to single hosts

Cons of SW:

- Gets a little tricky when trying to share with other devices on your networks
- Can be limiting depending on topology
- Requires a little under the hood work at times to implement
- At the mercy of the PC if running critical infrastructure

SBE.

TRANSMISSION TALK TUESDAY

Education

Good Morning.

To whom it may concern.

I want to make an enquiry but am confused on the exact person to contact. The email i contacted bounced back as failure delivery.

Please advice on the above need.

Thank You

Dear jwelton@nautel.com, Your password will expire in 24hours. To continue using your current password, please follow the link below.

Keep My Password

Note: Take action now or you will lose access to your emails and files.

Remediation efforts found that the cause of this detection was unauthorized software that had been previously installed on the computer. As per our Computer Usage Policy:

“Users may not install software onto their individual computers or the network without first receiving authorization to do so from IT…”

Microsoft

Sign in to view your fax / E1 Document

Your E1 fax is now available in the Microsoft inbox center. Sign in to view it. If you've already review, disregard this email.

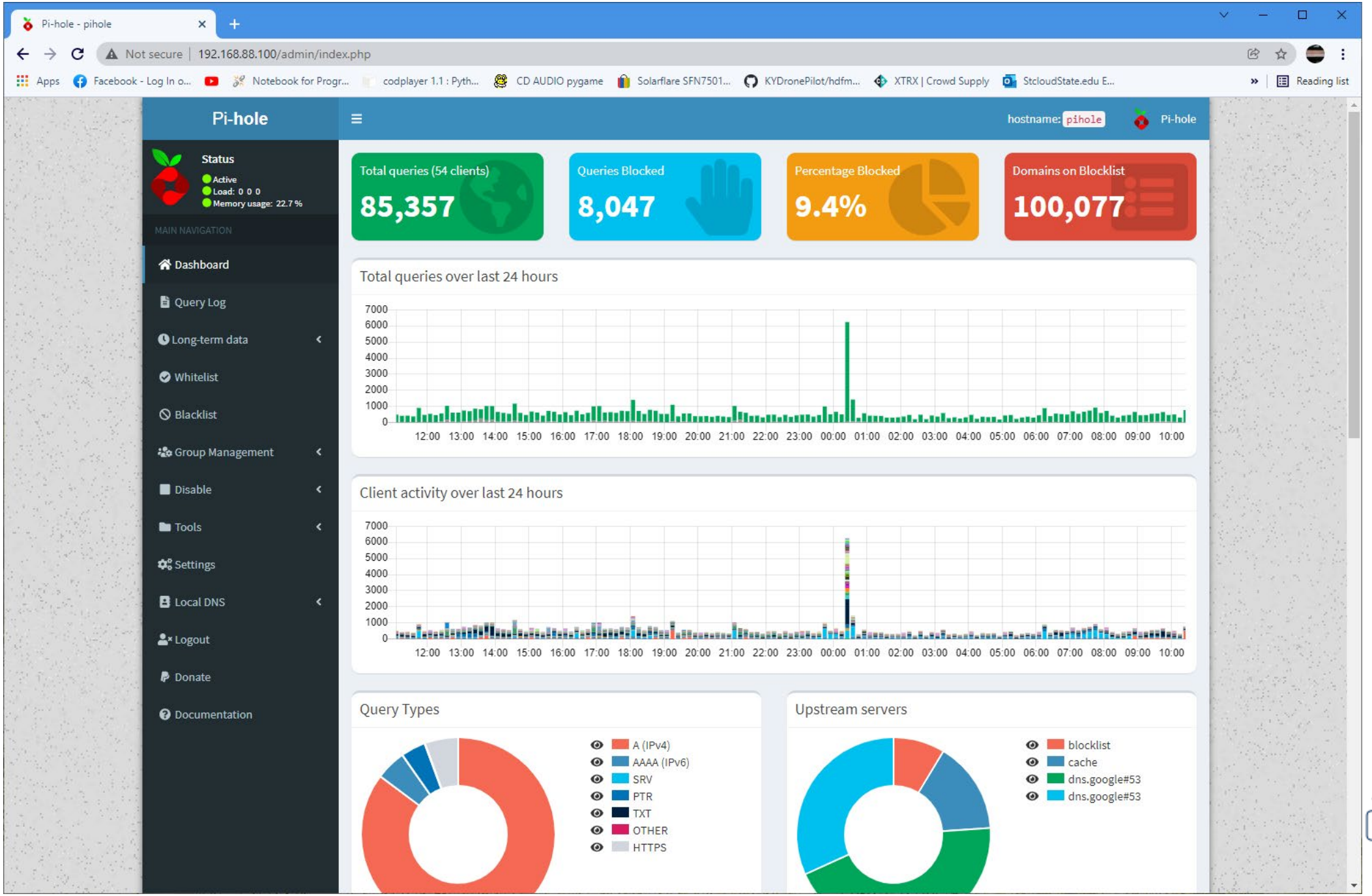
View your fax >

SBE.

TRANSMISSION TALK TUESDAY

I try to keep track of all the vulnerabilities, but it's getting harder and harder as time passes. RedHat alone sends out as many as a dozen reports a day; most are for minor bug fixes, but a few are true show-stoppers. As I write this, I just installed a newly-patched Linux kernel on our web server. All of those RedHat advisories made me suspect that it was time to upgrade. Indeed it was.

Stephen Poole, from Crawford Media Group's January engineering newsletter


Pi-hole - pihole
Not secure | 192.168.88.100/admin/index.php
Apps
Facebook - Log In o...
Notebook for Progr...
codplayer 1.1 : Pyth...
CD AUDIO pygame
Solarflare SFN7501...
KYDronePilot/hdfm...
XTRX | Crowd Supply
StcloudState.edu E...
Reading list
Pi-hole
hostname: pihole
Pi-hole
Status
Active
Load: 0 0 0
Memory usage: 22.7 %
MAIN NAVIGATION
Dashboard
Query Log
Long-term data
Whitelist
Blacklist
Group Management
Disable
Tools
Settings
Local DNS
Logout
Donate
Documentation
Total queries (54 clients)
85,357
Queries Blocked
8,047
Percentage Blocked
9.4%
Domains on Blocklist
100,077
Total queries over last 24 hours
7000
6000
5000
4000
3000
2000
1000
0
12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00
Client activity over last 24 hours
7000
6000
5000
4000
3000
2000
1000
0
12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00
Query Types
A (IPv4)
AAAA (IPv6)
SRV
PTR
TXT
OTHER
HTTPS
Upstream servers
blocklist
cache
dns.google#53
dns.google#53

Points to Ponder

Intrusion detection and prevention, active/stateful packet inspection, deep packet inspection

Don’t poke holes in the firewall!

Multiple entry points

Easy, cheap, reliable – pick any two

Backup, backup, backup!!!

https://www.cbtnuggets.com/

Online Information

Webinars
https://www.nautel.com/resources/webinars/

Nautel Waves Newsletter
https://www.nautel.com/newsletters/

YouTube
http://www.youtube.com/user/NautelLtd

Online Info, such as the Broadcasters' Desktop Resource
https://www.thebdr.net/

SBE.

TRANSMISSION TALK TUESDAY

THANK YOU!